Viewpoint Paper ■

Whose Personal Control? Creating Private, Personally Controlled Health Records for Pediatric and Adolescent Patients

Fabienne C. Bourgeois, MD, MPH, Patrick L. Taylor, JD, S. Jean Emans, MD, Daniel J. Nigrin, MD, MS, Kenneth D. Mandl, MD, MPH

Abstract Personally controlled health records (PCHRs) enable patients to store, manage, and share their own health data, and promise unprecedented consumer access to medical information. To deploy a PCHR in the pediatric population requires crafting of access and security policies, tailored to a record that is not only under patient control, but one that may also be accessed by parents, guardians, and third-party entities. Such hybrid control of health information requires careful consideration of both the PCHR vendor's access policies, as well as institutional policies regulating data feeds to the PCHR, to ensure that the privacy and confidentiality of each user is preserved. Such policies must ensure compliance with legal mandates to prevent unintended disclosures and must preserve the complex interactions of the patient-provider relationship. Informed by our own operational involvement in the implementation of the Indivo PCHR, we provide a framework for understanding and addressing the challenges posed by child, adolescent, and family access to PCHRs.

■ **J Am Med Inform Assoc.** 2008;15:737–743. DOI 10.1197/jamia.M2865.

Background

Personally controlled health records (PCHRs),[1] a subset of personal health records (PHRs),[2,3] enable individuals to aggregate, securely store, and access electronic health information from multiple sites of care, and to share that information with care providers and others.[4,5] Shared, ubiquitous, consent-modulated access to medical information promises reduced medical errors,[6] improved efficiency and safety of medical care,[7] and lower health care costs,[8–10] as well as activated patients who take responsibility and become partners in managing their own healthcare.[11]

As a possible central component of the Nationwide Health Information Network, an electronic infrastructure to promote the exchange of healthcare information[12,13] and improve the quality of healthcare, PCHRs have received considerable national attention. The key innovation of PCHRs is ensuring personal control over information access and use, which motivates patients to be active collaborators in the quality and continuity of their care by assembling, reviewing, and adding to clinical information.[14,15] They have therefore been treated as a key part of comprehensive visions for health care redesign, such as the Markle Foundations' Connecting for Healthcare and Project HealthDesign. At the same time, PCHRs have garnered attention from technology corporations, such as Microsoft and Google,[16,17] and from large companies seeking to provide PCHRs to their employees, such as Dossia.[18,19]

Just as an individual can use Quicken® to aggregate information from financial institutions, an individual can use the PCHR to "subscribe" to data from electronic health record systems, pharmacies, and laboratories.[20] Because consumers can grant access to their PCHR to others, institutions providing data subscriptions to PCHR platforms must be cognizant that in many cases the PCHRs will be used not just by individual adults, but by families, children, and adolescents. These institutions must give careful consideration to policies and principles governing access to the information and be mindful of their own responsibility for disclosing health information, as well as the policies and procedures of the PCHR platform vendor. These policies must ensure compliance with legal mandates, prevent unintended disclosures of

Affiliations of the authors: Division of General Pediatrics (FCB), Division of Emergency Medicine (KDM), Office of the General Counsel (PLT), Division of Adolescent Medicine (SJE), Information Services Department (DJN, KDM), Children's Hospital Informatics Program (DJN, KDM), Children's Hospital Boston, Boston, MA; Department of Pediatrics (FCB, PLT, SJE, DJN, KDM), Center for Biomedical Informatics (DJN, KDM), Harvard Medical School, Boston, MA.

This work was supported by R01 CDC 000065-01 and P01 CD000260-01 from the Centers for Disease Control and Prevention, by T32HP10018-12 from the Health Resources and Service Administration, and by Children's Hospital Boston.

The authors thank Mary Radley for comments on the manuscript.

Dr. Mandl reports receiving support from the nonprofit Children's Hospital Boston, a pediatric teaching hospital, to provide unrestricted and nonexclusive advice that informs the joint work between Children's Hospital Boston and the nonprofit entity Dossia, as well as other deployments of Indivo—an open-source, freely available PCHR—with respect to success factors for PCHR diffusion and the personal control model of health information. Dossia has a contract with Children's Hospital Boston that supports the use of Indivo by the employees of the Dossia founding companies. The core PCHR software produced under this contract is made freely available as part of the open-source code base of Indivo. No other potential conflict of interest relevant to this article was reported.

Correspondence: Fabienne C. Bourgeois, MD, MPH, Division of General Pediatrics, Children's Hospital Boston, 300 Longwood Avenue, Boston, MA 02115; e-mail: <fabienne.bourgeois@childrens.harvard.edu>.

Received for review: 05/19/08; accepted for publication: 08/15/08.

health information, and preserve the complex interactions of the patient-provider relationship.

Informed by our own operational involvement in the implementation of the Indivo PCHR at Children's Hospital Boston, we provide a framework for addressing the challenges posed by child, adolescent, and family access to PCHRs.

Personally Controlled Health Records in Pediatrics

To be a lifelong record, a PCHR must evolve with children and their families and accommodate the specialized needs of both. The PCHR will need to support healthcare and wellness management related to development, growth, and transitions from childhood to adolescence and adolescence to adulthood. All the while, the record must support the multiple participants in the child's health care management—not only patients and primary care providers, but also parents, guardians, relatives, school nurses, and perhaps social workers and specialists.

Challenges

This need for shared access poses significant challenges around protecting privacy and confidentiality for patients and families. Parents, guardians, and third-party entities, such as social service providers, may require access to the record in the course of care, and the patient's ability to understand and consent to such access varies with age and circumstances.

Unique health privacy and confidentiality standards apply where minors are concerned.[21,22] Privacy protection under the Health Insurance Portability and Accountability Act (HIPAA) in the pediatric context is especially complex, because extended proxy and hybrid access requires separate consideration of the rights of the different users, and the privacy expectations of the different record contributors.

Under certain conditions, the PCHR infrastructure must allow for some information to be accessible only to the parent, some only to the adolescent. Certain consent and privacy laws and court decisions allow minors to consent to particular kinds of health care without parental consent or notification, and explicitly or implicitly protect the privacy of those choices.[23] These situations may include visits for reproductive health, sexually transmitted diseases, psychiatric services, and for substance abuse and dependence, where the minor wishes the information kept confidential, and asserts the right to privacy or exercises specially recognized autonomy.

Other laws and decisions base the ability of minors to consent on their belonging to certain categories, which are loosely equated to personal and financial independence and adult status, such as situations where the minor is married, actively serving in the military, or financially independent of parents and living apart from them. Where statutes or case law support it, such minors are categorically capable of independently consenting to their own health care, or the health care of their own children. Minors' health information in these cases is considered confidential and cannot be shared with parents or guardians without the adolescent's consent, or under unusual circumstances.

To further complicate matters, there are extensive variations in state and local laws and statutes involving minor's rights to consent to their own health care, as well as in institutional interpretations of these laws.[24] For instance, the age of majority, at which point a person is considered an adult and may consent to and manage his or her own health care, varies among states. While most states set the age at 18 years, Nebraska and Alabama consider 19 the age of majority, but Alabama nonetheless allows health care consent by minors fourteen years of age and older. The intricacies involving abortion laws and reproductive health present even greater dissimilarities between states. Laws also vary regarding the role of an individual physician's discretion in disclosing sensitive information.

Information shared by a caregiver in confidence, such as statements regarding domestic abuse or parental depression, should also be protected. The parent may not want to share this information with the child or with another parent who may share custody and be otherwise entitled to access the child's medical records. Even the address of one parent may need to be protected from the other separated parent, and judgment may be required to identify situations in which precaution is required.

Parents may also not want to disclose particular health information to the minor, and request that healthcare providers refrain or delay sharing the information with the patient. In circumstances where the family is concerned about how the patient may cope with or be stigmatized by the disease, parents or guardians may ask to restrict access to this information from the child until she is older, or withhold information from extended family or care takers. In these situations the requests of the parents must be respected, although they may also trigger negotiation among the parents, clinicians, institutional ethicists, and counsel.

Furthermore, attention has to be paid to the content of the medical information provided, and how it is best delivered to the patient or patient's parents. Sensitive results, such as HIV results, prognoses, and genetic information, may need additional safeguards before being released into the record, to ensure the information is delivered in an appropriate manner and that it is released with parents' understanding and genuine consent. Other information may need a provider's explanation to avoid misinterpretation or to meet a reasonable expectation of health literacy and compassionate care. This type of sensitive information may be handled with a fixed embargo period before appearing in the record, or in some cases an institution might decide not to populate the PCHR with such data at all.

Thus an important distinction needs to be made in the conceptualization of a PCHR in the pediatric setting. Here, the PCHR is not purely patient controlled, but instead is controlled under a hybrid model, as the responsibility for a child's health care management shifts over time. The individual user's role and interaction with the record will differ over time to accommodate the evolving requirements dictated by the emerging developmental, legal, and intellectual maturity of the adolescent and young adult.

Addressing the Challenges

In considering potential solutions to the complex issues of pediatric access policies and privacy considerations for PCHRs, it is imperative to consider these challenges as they pertain to both institutional and commercial PCHRs, in

particular reconciling the potentially divergent requirements for institutional data subscriptions with user policies created by commercial vendors.

Specifically, two issues need to be distinguished. The first is the terms and conditions a PCHR requires of families and patients who wish to gain access to the record. These are the user access policies to which the patients and parents agree in order to create a PCHR account. The second issue is the provisions under which the PCHRs retrieve and manage institutional or practice-based medical records that supply data feeds to the PCHR; these are records that have been established according to laws, regulations, institutional policies, and local expectations of privacy.

User Access Policies: Considerations for Institutional and Commercial PCHRs

One can envision two opposite sides of a spectrum in handling the agreement between the PCHR and families concerning access and privacy. One solution might try to replicate individual institutional policies that are also supplying data to the PCHR, so that in effect the PCHR platform vendor is agreeing in advance with families that, in granting minors, parents, and others differential access, it will abide by institutional procedures from data-supplying institutions. This system would require the PCHR to comply with complex access policies and data downloads consistent with multiple institutions' legal and ethical standards for the protection of confidential health information. Whether tethered to an institution, or commercially sponsored, such a PCHR would be both complex and time-consuming, as it demands the creation, implementation, and enforcement of intricate policies and procedures that will no doubt vary in direct proportion to the multistate usefulness of a PCHR in gathering data from diverse sites of care. Further, it diminishes the true individual or family control over the information.

Alternatively, one can conceive of a simpler approach which may be more appealing to commercial PCHR providers. This scheme requires a contractual agreement from the patients and parents in which they simply waive the confidentiality between the family and the child, allowing equal access to medical records in the PCHR by the parent and the adolescent patient alike. This tactic would bypass the constraints imposed by institutional policies and would require less oversight and complex implementation strategies. However, this approach would impose a severe cost in that the price of PCHR participation would be waiving the very privacy rights that patients and families insist on in seeking care from institutions and medical practices.[21,25] It would therefore severely hamper efforts to spread PCHR access. Families unwilling to waive rights would not be provisioned a PCHR, and those that did waive the rights may have an impaired sense of trust, which would diminish the usefulness of the record, since patients and families would be incented to limit downloads that contain highly confidential but clinically vital information. Furthermore, some institutions, concerned about sensitive information made broadly available without careful thought or clinician discussion, would likely hesitate to participate, and perhaps insist on restricting the scope of their subscriptions to avoid clinically important but sensitive information. Additionally, the needs and rights of the adolescent patient would change over time, jeopardizing the continued legitimacy and applicability of the initial consent to waive confidentiality. For PCHRs to be a viable alternative to institutional records, they must credibly grapple with some of the same data sensitivity drivers that have led to current laws, regulations and institutional policies.

The approach we recommend walks a middle path, suggesting that access policies embody categorical protection, without guaranteeing that such policies will in all cases conform to the varying policies of providers supplying medical information to the PCHR (Tables 1 and 2). Parents and families would agree to these differential access policies through HIPAA-compliant authorizations at the time of account provisioning, allowing for the varying needs of the users and the changing need of the pediatric patient over time.

Policies for Institutional Downloads to the PCHR

In addition, procedures need to be established to regulate the institutional data available in subscriptions to the PCHR. The guidelines by which the PCHR retrieves institutional and practice-based data need to be continuously monitored to ensure that information is released to the proper users with the appropriate security levels. Implementing these procedures allows for different solutions requiring varying involvement of the individual institutions or commercial enterprises. These solutions must again balance the elegance of simplicity and uniformity of policies versus the complexity and flexibility demanded by institutional freedom and individual autonomy.

The first solution calls for the creation of an independent, non-healthcare, HIPAA-compliant entity that would create

Table 1 ■ Access Control Policies for a PCHR Based on Patient's Age

Patient's Age	Parent/Guardian Access	Patient Access	Registration
< 13 yrs	All medical information	None	Registration/Consent of parents; Screening by PCHR administrator.
13-<18 yrs	Most information, except sensitive/ confidential patient data*	Most information except sensitive parent and other 3rd party data*	Re-registration at age 13; consent by parent for access of information by teen; agreement by teen; confidentiality and sensitive test rules in place.
≥ 18 yrs	None, unless access rights to others granted by patient, law or court order	All medical information	Re-registration by adolescent to be sole owner of PCHR.

PCHR = personally controlled health records.
*Examples of sensitive data are shown in Table 3.

Table 2 ■ Pediatric PCHR Access Controls

	Age		
	<13 Years	13-<18 Years#	≥ 18 Years*
Indivo/Portal General Access	C− | P+	C+ | P+	C+
Problem List	C− | P+	C+ | P+ except	C+
Sensitive Dx that parent cannot access†		C+ | P−	
Sensitive Dx that patient cannot access‡		C− | P+	
Procedure List	C− | P+	C+ | P+ except	C+
Sensitive Proc. that parent cannot access†		C+ | P−	
Medication	C− | P+	C+ | P+ except	C+
Sensitive Meds that parent cannot access†		C+ | P−	
Allergies	C− | P+	C+ | P+	C+
Immunizations	C− | P+	C+ | P+	C+
Clinic Notes	C− | P+	C+ | P+ except	C+
Sensitive info that parent cannot access†		C+ | P−	
Sensitive info that patient cannot access‡		C− | P+	
Laboratory Results	C− | P+	C+ | P+ except	C+
Sensitive tests that parent cannot access†	C− | P−	C+ | P−	
Sensitive tests that child cannot access‡		C− | P+	
Genetics		C− | P+	
Radiology Results	C− | P+	C+ | P+ except	C+
Sensitive tests that parent cannot access†		C+ | P−	
Sensitive tests that patient cannot access‡		C− | P+	
Pathology Results	C− | P+	C+ | P+ except	C+
Sensitive result that parent cannot access†		C+ | P−	
Sensitive result that patient cannot access‡		C− | P+	

C = Child/Adolescent Patient; P = Parent/Guardian; PCHR = personally controlled health record; + = access allowed; − = access not allowed.

*Access allowed to parent/guardian only if patient allows or if parent has been legally declared medical guardian for adolescents ≥18. It is also recognized that age of consent is higher in several states.

†Without agreement of patient.

‡Without agreement of parent.

#General access to medical information granted to minor adolescent patient provided the parent/guardian consents. Access to patient's sensitive information granted regardless of parental consent.

and oversee uniform standards that address all situations, including variations in state laws. Such an entity would be able to enforce and regulate how information is downloaded into the PCHRs and would be able to control the data objectively, while accepting the responsibility to address coherence and consistency of the policies. However, such an entity would be difficult to create, as it would require a consensus upon the interpretation of laws and statutes, amending diverging state and local laws, and creating uniform, somewhat dictatorial standards for physicians. This solution would thus undermine individual and institutional freedom to frame care in response to patient needs and the local culture of care.

Alternatively, institutions would themselves have to set up procedures to engage with the PCHR and create institutional access policies that would be mindful of legal and institutional procedures and requirements. These policies would refine institutional data subscriptions to the PCHR consistent with patient expectations about how the institution will maintain the privacy of clinical records. Such a solution requires the institutions to individually manage the inherent complexity of rules governing pediatric health information, and would differ among institutions, requiring institutions to have some mechanism, such as a privacy officer, to resolve situations where complications or difficulties arise. This framework also places the greatest burden of responsibility on the individual providers and institutions to protect the patient's privacy.

The third option, and the one we recommend, is to have categorical policies for institutional subscriptions that replicate precisely the access policies that patients and families agree to in setting up a PCHR account and that shift during the developmental trajectory of the young patient. This allows the PCHR to tell data-supplying institutions across states that they need not be concerned about their own policies. Patients and families, empowered by the PCHR, have agreed to abide by categorically protective rules and have adjusted their expectations about how institutional and provider records would be protected to conform to the PCHR rules. This solution provides necessary uniformity, where there may be none among institutions, especially in different states, but is protective of patient and family rights and confidentiality, rather than being a general waiver. It is also implementable—if PCHR providers solicit member enrollment through terms and conditions that meet the HIPAA requirements for an authorization, institutions will be able to rely on that authorization to release protected health information to the PCHR.

Institutions will have to identify and label protected health information as sensitive, either by creating a standardized institutional list that complies with federal and state laws and reflects institutional policies, or, by allowing certain data elements in an electronic health record, such as certain potentially sensitive laboratory results or radiology results, to have a "checkbox" that allows the clinician to decide on a case by case basis whether to share that particular data with

the patient/family. Although this degree of customization allows for tailoring of what data are shared in each situation, it also essentially ensures that (1) mistakes will be made in what is shared/not shared, and that (2) since clinician input is needed, and clinician views about what is sensitive may vary, data sharing may be inconsistent, both among clinicians and compared to family or PCHR holder expectations. Furthermore, this could lead to delays in the release of information, as it requires the clinician to review the results first. The institution could also tag individual data elements as viewable by only the parent, only the adolescent or by both. The PCHR would need to maintain that label attached to the data as a core attribute. Hence, the institutional interpretations of data as sensitive or appropriate for access by certain parties would become bound to the data, and the PCHR would need to act on those attributes consistently in perpetuity.

Should a PCHR platform vendor choose not to provide differential user access policies that honor the privacy rights and confidentiality of the adolescent patient and other users, the burden would reside with the institution to protect against unwanted disclosures. This may necessitate agreements between the vendors and institutions, where institutions may restrict or limit downloads of protected health information to the PCHR if the appropriate safeguards are not supported by the PCHR viewer access policies.

Coming of Age

Vendors of PCHR platforms will also need to implement a change in access policies when a user turns 18. Implementing this shift, to provide sole access to the patient and restrict access to the existing record by other users, poses significant challenges. While institutions may terminate additional new data feeds to the PCHR on the day the patient turns 18, thus preventing access to new health information by all users, it is the PCHR vendor that must appropriately disable parental or other third-party accounts.

The system could mirror a paper record system in which family members and others given proxy access to the record would continue to have access to the health information they previously had access to in perpetuity, even after the user turns 18. Access to future data could be shut off for proxy users, and need to be reestablished by the patient. Alternatively, access could be terminated completely when the patient turns 18, preventing parents and guardians from accessing the record altogether, including the childhood record, without the patient's consent.

Model Access Policy Framework

For the roll-out of our institutionally-based PCHR, the Indivo record,[20,26] accessed through the www.MyChildrens.org portal at Children's Hospital Boston, we generated a set of access policies and rules governing data downloads that were guided by our institutional principles and policies, and are also designed to respect the complex privacy needs dictated by pediatric health information.

Account Provisioning

We created a mechanism to authenticate the parents or guardians during the registration process to ensure their legal status as the patient's guardian. Although semi-automated, this process involves manual human review of every application for an account and for proxy access to a child's record. All changes to the role of the legal guardian, including situations where the parent retains legal and medical guardianship after a child turns 18, will be handled by a PCHR administrator. Minor patients will be granted access to their medical information starting at age 13 years, provided parents or guardians give their consent (Table 1). However, even if parents do not wish to grant their adolescent children general access to medical information, patients will still be able to create an account and access certain sensitive medical information (Tables 1 and 2). Our process also requires a re-registration process by the patient at each of the pivotal age categories.

User Access

We identified three subpopulations within the pediatric patient population that need to be considered separately when establishing access control policies and rules. These subpopulations were established based on age-defined developmental maturity, as well as generalized state laws governing minor's rights to consent to their healthcare in certain situations (Table 1). Furthermore, we identified the specific content of the medical record requiring differential access based on the three subpopulations (Table 2). In addition, we identified sensitive test results requiring differential access, as well as results that we felt were best communicated by a provider directly to a patient and/or parent, such as pathology or radiology results for cancer diagnoses, or a new genetic diagnosis, and established exclusions or specific time delays before the results are available in the PCHR (Table 3). The delay allows the time for the provider to review the results and directly communicate the findings to the patient and family with the appropriate counseling. Further studies involving patients, parents, and providers will be necessary to further refine this list.

Existing implementations of patient portal systems such as PatientSite,[27,28] MyHealth*e*Vet[29] and Epic's MyChart do not allow patients to read clinical notes; however, we see great value enabling the patient to make these notes available to care providers who may wish to use the record as a secondary data source for clinical decision making or for patients who may wish to review or verify the treatment plan. We recognize that there may be information documented that is not intended to be shared with the patient or the family. While patients and families already have access to these notes through a request for medical records, making them readily available electronically qualitatively and quantitatively changes the nature of this access. Hence, we include only notes created by providers after the date the system has gone live. Furthermore, we are exploring options to appropriately handle confidential information included in the documents, such as creating a separate confidential section of the note that can be routed to the appropriate user, for example, only to the adolescent patient if, as part of her visit, she had a consultation regarding birth control, or potentially a sophisticated natural language processing system to identify sensitive information, thereby protecting confidential disclosures made by the adolescent patient, family members, or third-parties. We will also need to ensure that third-party disclosures made in confidence are properly addressed once the patient turns 18 and gains full

Table 3 ■ Examples of Sensitive Results Requiring Special Consideration

Laboratory Results
Infectious Disease
Chlamydia Trachomatis
Neisseria Gonorrhoeae
Hepatitis B Virus
Hepatitis C Virus
HIV ELISA/Western Blot
HIV Viral Loads
HIV Phenotype
CD4 count
Human Papilloma Virus
Herpes Simplex Virus
Rapid Plasma Reagin
Trichomonas
Toxicology
Amphetamine
Barbiturates
Benzodiazepine
Cannabinoid
Cocaine
Ethyl alcohol
Methamphetamine
Opiate
Phencyclidine
Genetics
All genetic test results
Reproductive Health
Pregnancy test (HCG)
Alpha-Fetoprotein
Immunology
Human Leukocyte Antigen typing
Radiology Results
Pelvic Ultrasound related to Pregnancy
Pathology Results
Products of conception
Pap Test

access to his or her medical record, including information that was withheld while the record was also controlled by the parent.

Conclusion

Access control policies for a PCHR need to handle developmental and age-defined rights of users to preserve privacy, confidentiality, and best interests. This requires rules specifying separate access to sensitive information for adolescent patients and parents, as well as embargoes on results best delivered by providers themselves. Information sharing for the adolescent patient, where alternative rules are important, requires review to choose access policies that reasonably conform to local laws, court decisions, professional society guidelines, patients' and families' privacy and informational expectations, and clinicians' judgments about how to communicate information that meets patients' health literacy and standards of compassionate care. We advocate a moderate approach that addresses the values and requirements of federal, state and local statutes, individual institutions, providers' clinical judgment, as well as the needs of the individual, while avoiding extremes that would doom the PCHR effort to empower patients and families to access and control their health information in the highly networked environment. Subsequent stages of PCHR development will involve refining these rules, to take into account multiple institutional and other providers own tolerances for record-sharing on these terms, and patients' and families' own evolving sensibilities and the impact on PCHR utilization of policy changes. Allowing customization and fine-tuning of access controls, as well as creating privacy officers and other mechanisms to resolve complex situations and harmonize PCHR policies with provider privacy practices will best preserve the privacy needs of minors and their families and hence capacitate the PCHR infrastructure to serve their healthcare needs.

References ■

1. Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ 2001;322(7281):283–7.
2. Halamka JD, Mandl KD, Tang PC. Early Experiences with Personal Health Records. J Am Med Inform Assoc, 2008;15(1): 1–7.
3. Pagliari C, Detmer D, Singleton P. Potential of electronic personal health records. BMJ 2007;335(7615):330–3.
4. Mandl KD, Kohane IS. Tectonic shifts in the health information economy. N Engl J Med, 2008;358(16):1732–7.
5. Steinbrook R. Personally controlled online health data–the next big thing in medical care? N Engl J Med, 2008;358(16):1653–6.
6. Feied CF, Handler JA, Smith MS, et al. Clinical information systems: instant ubiquitous clinical data for error reduction and improved clinical outcomes. Acad Emerg Med. 2004;11(11): 1162–9.
7. Mahoney CD, Berard-Collins CM, Coleman R, Amaral JF, Cotter CM. Effects of an integrated clinical information system on medication safety in a multi-hospital setting. Am J Health Syst Pharm, 2007;64(18):1969–77.
8. Baker LC. Benefits of interoperability: a closer look at the estimates. (Suppl Web Exclusives) Health Aff (Millwood), 2005: W5-22–W5-25.
9. Walker J, Pan E, Johnston D, Adler-Milstein J, Bates DW, Middleton B. The value of health care information exchange and interoperability. (Suppl Web Exclusives). Health Aff (Millwood), 2005:W5-10–W5-18.
10. Hook JM, Pan E, Adler-Milstein J, Bu D, Walker J. The value of healthcare information exchange and interoperability in New York state. AMIA Annu Symp Proc, 2006:953.
11. Teich JM. The benefits of sharing clinical information. Ann Emerg Med. 1998;31(2):274–6.
12. Leavitt lays the groundwork for NHIN standards. HHS touts public-private collaboration for HIT interoperability. Med Health, 2005;59(20):4.
13. Connecting For Health: A Public-Private Collaborative. The Personal Health Working Group Final Report. July 1, 2003, The Markle Foundation.
14. Harvard Medical School Meeting on Personally Controlled Health Record Infrastructure 2006. 2006. Available at: http://www.pchri.org/2006. Accessed on September 10, 2008.
15. Harvard Medical School Meeting on Personally Controlled Health Record Infrastructure 2007. 2007. Available at: http://www.pchri.org/2007. Accessed on September 10, 2008.
16. Lohr S. Microsoft Rolls Out Personal Health Records. The New York Times. 2007.
17. Lohr S. Google and Microsoft Look to Change Health care. The New York Times. 2007.
18. McGee MK. Intel, Wal-Mart, And Others Refocus to Get Worker E-Health Record System Running. Intelligent Enterprise, 2007.
19. McWilliams G. Employers Back Development of Web-Based Health Record. The Wall Street Journal. September 17, 2007.

20. Mandl KD, Simons WW, Crawford WC, Abbett JM. Indivo: a personally controlled health record for health information exchange and communication. BMC Med Inform Decis Mak. 2007;7:25.
21. Ford C, English A, Sigman G. Confidential Health Care for Adolescents: position paper for the society for adolescent medicine. J Adolesc Health, 2004;35(2):160–7.
22. Informed consent, parental permission, and assent in pediatric practice. Committee on Bioethics, American Academy of Pediatrics. Pediatrics 1995;95(2):314–7.
23. Berger JE. Consent by proxy for nonurgent pediatric care. Pediatrics 2003;112(5):1186–95.
24. Vukadinovich DM. Minors' rights to consent to treatment: navigating the complexity of State laws. J Health Law 2004;37(4):667–91.
25. van Straaten J. The minor's limited right to confidential health care and the inverse of confidentiality: a parent's decision not to disclose illness status to a minor child. Child Leg Rights J. 2000;20(1):46–54.
26. Simons WW, Mandl KD, Kohane IS. The PING personally controlled electronic medical record system: technical architecture. J Am Med Inform Assoc 2005;12(1):47–54.
27. Weingart SN, Rind D, Tofias Z, Sands DZ. Who uses the patient internet portal? The PatientSite experience. J Am Med Inform Assoc, 2006;13(1):91–5.
28. Sands DZ. Personal Communication. 2007.
29. Morgan MW. The VA advantage: the gold standard in clinical informatics. Healthc Pap 2005;5(4):26–9.